## Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

1. (currently amended)    A method comprising: fabricating a first plurality of FPGA integrated circuits with a first secret key embedded by way of a first mask set; and fabricating a second plurality of FPGA integrated circuits with a second secret key embedded by way of a second mask set; and wherein loading an unencrypted bitstream is loadable into one of the first plurality of FPGA integrated circuits to generate a secure bitstream using the first secret key; wherein a the first secure bitstream will configure properly user-configurable logic of the first plurality of FPGA integrated circuits, but not the second plurality of FPGA integrated circuits.

2-3. (cancelled)

4. (original)   The method of claim 1 wherein the first plurality of FPGA integrated circuits with the first secret key are assigned to a first geographic area and the second plurality of FPGA integrated circuits with the second secret key are assigned to a second geographic area.

5. (original)   The method of claim 1 wherein the first plurality of FPGA integrated circuits with the first secret key are fabricated in a first time period and the second plurality of FPGA integrated circuits with the second secret key are fabricated in a second time period, different from the first time period.

6. (original)   The method of claim 1 wherein only one mask differs between the first and second mask sets.

7. (original)   The method of claim 1 wherein the first plurality of FPGA integrated circuits with the first secret key are assigned exclusively to a first customer.

8. (original)   The method of claim 5 wherein the first time period is about the same duration as the second time period.

9. (original)   The method of claim 5 wherein the first time period is a different duration from the second time period.

10 (original)   The method of claim 6 wherein the one mask is a contact mask.

11. (original)  The method of claim 1 wherein there are random differences between artwork of the first and second plurality of FPGA integrated circuits in addition to the different embedded secret keys.

12. (original)  The method of claim 1 wherein the first and second secret keys are presented on wires of respective plurality of FPGA integrated circuits for only a limited duration.

13. (original)  The method of claim 1 wherein the first secret key is embedded by setting an initial state of a selection of memory cells in a device configuration memory of the FPGA integrated circuit.

14. (original)  The method of claim 1 wherein the first secret key is embedded by changes to a relatively large block of logic in the first plurality of FPGA integrated circuits and its value extracted using a CRC algorithm.

15. (original)  The method of claim 13 further comprising: extracting the first secret key by using a CRC algorithm to compute a checksum of the initial state of the device configuration memory.

16. (currently amended)    The method of claim 1 ~~further comprising:~~ wherein ~~loading~~ an unencrypted bitstream is loadable into one of the first plurality of FPGA integrated circuits to generate a secure bitstream based on the first secret key and an on-chip generated random

3

number.

17. (currently amended)    The method of claim 1 ~~further comprising:~~ wherein ~~loading~~ an unencrypted bitstream is loadable into one of the first plurality of FPGA integrated circuits to generate a secure bitstream based on the first secret key and an on-chip generated random number, wherein the secure bitstream includes a message authentication code.

18. (currently amended)    A method comprising: providing an FPGA integrated circuit having ~~embedding~~ a first secret key embedded within the artwork of ~~an~~ the FPGA integrated circuit; storing a user-defined second secret key within an encrypted FPGA bitstream stored in an external nonvolatile memory accessible by the FPGA; decrypting the user-defined second secret key using the first secret key; and setting up a secure network link between the FPGA and a server using the user-defined second secret key.

19. (original) The method of claim 18 further comprising: downloading an FPGA bitstream using the secure network link; encrypting the downloaded FPGA bitstream using the first secret key; and storing the encrypted downloaded bitstream in the external memory.

20. (original) The method of claim 18 wherein the secure network link is created using a standard internet security protocol.

21. (original) The method of claim 18 further comprising: configuring the FPGA using the encrypted downloaded bitstream stored in the external memory.

22. (currently amended)    A method comprising: storing a first secret key on an FPGA chip; causing the FPGA chip to calculate a message authentication code (MAC) corresponding to a user design; and storing the message authentication code with bitstream information in a nonvolatile memory.

23. (original)  The method of claim 22 further comprising: storing copyright messages with the bitstream information; detecting unauthorized alterations to the bitstream using the message authentication code; and preventing bitstreams which have been altered from being used to configure an FPGA.

24. (original)  The method of claim 22 further comprising: recording the message authentication code along with corresponding identification information for a product containing the FPGA; and examining the message authentication code stored in the nonvolatile memory of a product containing a pirated FPGA design, which will enable determining the identity of the customer to whom the pirated FPGA was originally supplied using a record of MACs and corresponding product identification.

25. (currently amended)     A method comprising:

fabricating a first plurality of programmable integrated circuits with a first secret key embedded by way of a first mask set; and

fabricating a second plurality of programmable integrated circuits with a second secret key embedded by way of a second mask set, wherein the second plurality of programmable integrated circuits comprise the same programmable logic as in the first plurality of programmable integrated circuits; and

wherein loading an unencrypted bitstream is loadable into one of the first plurality of programmable integrated circuits to generate a secure bitstream using the first secret key;

wherein a first the secure bitstream will configure properly user-configurable logic of the first plurality of programmable integrated circuits, but not the second plurality of programmable integrated circuits.

26-27. (cancelled)

28. (previously presented)    The method of claim 25 wherein the first plurality of programmable integrated circuits with the first secret key are assigned to a first geographic area

and the second plurality of programmable integrated circuits with the second secret key are assigned to a second geographic area.

29. (previously presented)    The method of claim 25 wherein the first plurality of programmable integrated circuits with the first secret key are fabricated in a first time period and the second plurality of programmable integrated circuits with the second key are fabricated in a second time period, different from the first time period.

30. (previously presented)    The method of claim 25 wherein only one mask differs between the first and second mask sets.

31. (previously presented)    The method of claim 25 wherein the first plurality of programmable integrated circuits with the first secret key are assigned to a first customer and the second plurality of programmable integrated circuits with the second key are assigned to a second customer.

32. (previously presented)    The method of claim 29 wherein the first time period is about the same duration as the second time period.

33. (previously presented)    The method of claim 29 wherein the first time period is a different duration from the second time period.

34. (previously presented)    The method of claim 30 wherein the one mask is a contact mask.

35. (previously presented)    The method of claim 25 wherein there are random differences between artwork of the first and second plurality of programmable integrated circuits in addition to the different embedded secret keys.

36. (currently amended)     The method of claim 25 wherein the first and second secret keys are <u>configured to be</u> presented on wires of <u>the</u> respective <u>first and second pluralities</u> ~~plurality~~ of programmable integrated circuits for only a limited duration.

37. (previously presented)     The method of claim 25 wherein the first secret key is embedded by setting an initial state of a random selection of memory cells in a device configuration memory of the programmable integrated circuit.

38. (currently amended)     The method of claim 37 ~~further comprising:~~ <u>wherein</u> ~~extracting~~ the first secret key <u>is extractable</u> by using a CRC algorithm to compute a checksum of the initial state of the device configuration memory.

39. (currently amended)     The method of claim 25 ~~further comprising:~~ <u>wherein</u> ~~loading~~ an unencrypted bitstream <u>is loadable</u> into on<u>e</u> of the first plurality of programmable integrated circuits to generate a secure bitstream based on the first secret key and an on-chip generated random number.

40. (currently amended)     The method of claim 25 ~~further comprising:~~ <u>wherein</u> ~~loading~~ an unencrypted bitstream <u>is loadable</u> into on<u>e</u> of the first plurality of programmable integrated circuits to generate a secure bitstream based on the first secret key and an on-chip generated random number, wherein the secure bitstream includes a message authentication code.

41. (currently amended)     The method of claim 25 ~~further comprising:~~ <u>wherein</u> ~~downloading~~ a secure programmable integrated circuit bitstream <u>is downloadable</u> through a network; and

~~configuring~~ one of the first plurality of programmable integrated circuits <u>is configurable</u> using the secure programmable integrated circuit bitstream by decoding the secure programmable integrated circuit bitstream using the first secret key.

42. – 47.  (cancelled)

48.  (previously presented)    A method comprising: storing a first secret key on an FPGA chip; using the first secret key and a user design to calculate a message authentication code (MAC) corresponding to the user design; and storing the message authentication code with bitstream information in a nonvolatile memory.

49.  (previously presented)    The method of claim 48 further comprising: storing copyright messages with the bitstream information; detecting unauthorized alterations to the bitstream using the message authentication code; and preventing bitstreams which have been altered from being used to configure an FPGA.

50.  (previously presented)    The method of claim 48 further comprising: recording the message authentication code along with corresponding identification information for a product containing the FPGA; and examining the message authentication code stored in the nonvolatile memory of a product containing a pirated FPGA design, which will enable determining the identity of the customer to whom the pirated FPGA was originally supplied using a record of MACs and corresponding product identification.